Mark Ravis (SBN: 137479)
mravis99@gmail.com
David Martin (SBN: 189755)
dhmartin99@gmail.com
Ivo Genchev (SBN: 285844)
LAW OFFICE OF MARK RAVIS & ASSOCIATES
1875 Century Park East, Suite 700
Los Angeles, California 90067
Telephone: 310-295-4145
Fax: 310-388-5251

Attorneys for Plaintiff ADELA GONZALEZ

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

ADELA GONZALEZ, on behalf of herself and all others similarly situated,

Plaintiff,

v.

BERKSHIRE HATHAWAY HOMESTATE COMPANIES, a Nebraska Corporation; CYPRESS INSURANCE COMPANY, a California Corporation; ZENITH INSURANCE COMPANY, a California Corporation; WILLIAM REYNOLDS, an individual; OLIVER GLOVER, an individual; HQSU SIGN-UP SERVICES, INC., a California Corporation and DOES 1 to 10, inclusive,

Defendants.

CASE NO: 16-2690

CLASS ACTION COMPLAINT FOR RELIEF BASED ON:

(1) Violation of the Computer Fraud and Abuse Act (18 U.S.C. §1030 et seq.)

(2) Violation of Unlawful Access to Stored Communications Act (18 U.S.C. §2701 et seq.)

(3) Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§2510 et seq.

(4) Invasion of Privacy (Public Disclosure of Private Facts)

(5) Intentional Interference with Prospective Economic Advantage

(6) Violation of the California Computer Data Access and Fraud Act (Cal. Penal Code §502 et seq.)

(7) Violation of California Business and Professions Code §17200

(8) Conversion

(9) Negligence

(10) Violation of the California Confidentiality of Medical Information Act (Cal. Civ. Code §56, et seq.)

(11) Violation of California Data Security and Breach Notification Act (Cal. Civ. Code §1798.80, et seq.)

DEMAND FOR JURY TRIAL

CLASS ACTION

COMPLAINT

SUMMARY OF THE CASE

1. Defendants Berkshire Hathaway Homestate Companies ("Berkshire Hathaway" or "BHHC"), Cypress Insurance Company (Cypress") and Zenith Insurance Company ("Zenith") and the other named hacking defendants illegally accessed and downloaded privileged and confidential litigation files of thousands of individuals litigating cases against them. The hacking defendants stole these files from servers used by law firms representing the individual litigants. BHHC, Cypress and Zenith are major worker's compensation insurance companies doing business in California and nationwide and many of the files were for workers compensation

litigants.

2. The defendants acted in complete disregard of constitutional and statutory law and applicable ethical and moral standards. Their corrupt conduct evidenced a total disregard for fair play and disregard for the integrity of the judicial system.

3. The hacking defendants are presently known to have hacked in excess of 32,000 litigation files.

4. Defendants' illegal hacking of privileged documents undermines the integrity of the judicial system which damages all Americans. The American system of justice depends upon fair play in an impartial forum. A fair and impartial forum for rich and poor alike is central feature of the American way of life and is important to our national reputation. This lawsuit is directed against those powerful insurance companies and their co-conspirators who because of their immense wealth and power acted as if they were above the law and in total disdain of our cherished concept of fair play in an impartial forum. The hacking defendants each conspired with one another, and aided and abetted one another, to break the laws set forth in this Complaint regarding computer security, confidential information and privacy.

5. Plaintiff is a client of the law firm of Reyes & Barsoum LLP who was pursuing a worker's compensation lawsuit on her behalf. She brings this proposed nationwide class action lawsuit on behalf of both Reyes & Barsoum clients

and other similarly situated clients whose privileged litigation files, with personal information, have been compromised as a result of the intentional data breach by defendants. Plaintiff seeks compensatory, statutory and punitive damages, as well as injunctive relief requiring defendants to refrain from all illegal computer intrusions.

PARTIES

6. Plaintiff Adela Gonzalez is a resident of Los Angeles County, California. Plaintiff's personal identifying information was compromised when the Hacking Defendants accessed HQSU servers, including but not limited to her full name, Social Security Number, birth date, home address, legal status, driver's license information, salary information, medical information and confidential legal information. To date, Plaintiff Gonzalez has expended hours and hours attempting to safeguard herself and her family members from identity theft or other harms caused by the release of her personal identifying information as a result of the cyberattack. Going forward, Plaintiff Gonzalez anticipates spending considerable time each day in an effort to contain the impact of the stealing of her personal identifying information on herself and her family members. Plaintiff's workers compensation case was also compromised because privileged and confidential information relating to her case was accessed and downloaded – the intent of the Hacking Defendants.

7. Defendant Berkshire Hathaway is a Nebraska corporation with its principal place of business in Omaha, Nebraska.

8. Defendant Cypress Insurance Company ("Cypress") is a California corporation and a wholly-owned subsidiary of Berkshire Hathaway Homestate Companies. Its principal place of business is San Francisco, California.

9. Defendant Zenith Insurance Company ("Zenith") is a California corporation with its principal place of business in Woodland Hills, California.

10. Defendant William Reynolds ("Reynolds") is an investigator who at one time was employed by Defendant Berkshire Hathaway and continues to hold himself out as an employee and/or agent of Berkshire Hathaway. He is a resident of the State of California.

11. Defendant Oliver Glover ("Glover") is an employee of Zenith Insurance Company and is a resident of the State of California.

12. Defendants Berkshire Hathaway, Cypress, Zenith, Reynolds, and Glover are collectively referred to as the "Hacking Defendants".

13. Defendant HQSU Sign Services, Inc. is a California corporation with its principal place of business located at 1609 East Palmdale Blvd. Suite D, Palmdale, California 93550. HQSU's president and registered agent for service of process is Carlos Humberto Morales. At all times relevant to this Complaint, HQSU maintained substantial and continuous contacts in the State of California and within the Central District in particular, and the acts and omissions giving rise to the claims against HQSU arise out of the acts and omissions occurring within the jurisdiction and venue of this Court.

14. Plaintiff does not know the true names and capacities of defendants sued herein as Does 1 to 10, inclusive, and therefore sues these defendants by such fictitious names. Plaintiff will amend this complaint to allege their true names and capacities when ascertained. However, on information and belief, Does 1 to 10 were/are the agents or employees or co-conspirators of each of the other defendants and are/were at all times relevant acting within the purpose and scope of such agency, employment, or conspiracy.

15. All of the defendants, named and unknown, are legally responsible either directly or vicariously (under theories of agency, conspiracy, or aiding and abetting) for all of the illegal constitutional, statutory, and tortious conduct alleged in this Complaint.

JURISDICTION AND VENUE

16. Jurisdiction is proper in this court because this litigation arises under federal law, including 18 U.S.C. §1030, et seq. ("Computer Fraud and Abuse Act"), 18 U.S.C. §2701, et seq. ("Stored Communication Act"), and 18 U.S.C. §§2510, et seq. ("Electronic Communications Privacy Act"). The Court has jurisdiction over this action under 28 U.S.C. § 1331 (federal question). The court also has jurisdiction over the state claims pursuant to its pendant and ancillary jurisdiction power.

17. This Court has personal jurisdiction over defendants as they each are

registered to conduct business in California, have sufficient minimum contacts in California, or otherwise intentionally avail themselves of the markets within California, through the promotion, sale, marketing and distribution of their products in California, to render the exercise of jurisdiction by this Court proper and necessary. Defendants Cypress and Zenith are incorporated in California.

18. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b) and 1391(c) because Plaintiff resides in this District, Defendants conduct substantial business in this District, and a substantial part of the events giving rise to plaintiff's claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

Plaintiff's Electronically-Stored, Privileged Litigation Files

19. Defendants BHHC, Cypress, and Zenith are among the largest providers of worker's compensation insurance in the United States. Together they provide a significant percentage of the worker's compensation insurance in California. These firms hired investigators who hacked into and stole stored confidential attorney-client files including files in which they were the insurer. Thousands of files have been pilfered and used by defendants in contravention of federal and state statutory law, case law, and standards of professional conduct.

20. The law firm of Reyes & Barsoum LLP specializes in worker's compensation, normally representing injured workers. Reyes & Barsoum contracted with HQSU to provide administrative services for clients unable to come to the

office due to physical, financial, or transportation limitations. HQSU maintained the servers on which personal client data was stored and on which the litigation files were stored.

21. HQSU is paid a pre-negotiated flat fee. HQSU represented to clients and agreed that it would keep clients' – including Plaintiff's – information secure and confidential.

22. In the case of Reyes & Barsoum clients, the accepting attorney informs the client that they will be contacted by HQSU for the purpose of signing a retainer agreement and filling out an In-Take Packet with personal information. HQSU then uploads the documents to its username and password-protected website. The information on this website is only available to Reyes & Barsoum attorneys following verification of username and password. Reyes & Barsoum may download existing documents, upload additional documents, and leave notes and comments related to the cases in the files stored for it by HQSU. This practice is used by all the other attorneys using the HQSU services.

23. Unbeknownst to Reyes & Barsoum or Plaintiff, and contradicting HQSU's assurances to the contrary, HQSU failed to provide adequate or responsible protections against unlawful access to the confidential and privileged it stored. Moreover, following the other Defendants' unlawful accessing and converting the data, as alleged below, HQSU failed to report the hacking activity to Plaintiff,

Reyes & Barsoum, other law firms using its services or the approximately 33 000 class members which information such as Social Security numbers, home addresses, telephone numbers, legal statuses, drivers licenses information, medical information, employment information was taken. In addition HQSU failed to inform law enforcement or appropriate government oversight agencies.

The Discovery of the Hacking Defendants' Unlawful Computer Hacking

24. The Hacking Defendants' hacking of the HQSU files was first suspected during an in-chambers hearing in a worker's compensation case before Presiding Judge Paige Levy. The hearing involved defense motions to compel further testimony of Applicant Hector Casillas and an HQSU employee, Chantelle Obregon, on April 20, 2014 in the matter of Hector Casillas vs. Xeres Corp; Broadspire Claims Services, WCAB NO. ADJ903073.

25. At the in-chambers conference, Knox Ricksen's attorneys revealed they had Mr. Casillas' attorney-privileged In-Take Packet which bore the name "ATTORNEY: Rony M. Barsoum, Esq." at the top of the document's first page as well as the Reyes & Barsoum Retainer Agreement signed by Mr. Casillas.

26. Judge Levy immediately asked Knox Ricksen's attorney how he came into possession of Mr. Casillas' In-Take packet. The attorney first responded that it was obtained from the HQSU "website". The attorney then changed his story and told Judge Levy that Ms. Obregon, HQSU's representative, had provided it to defendant. Finally, the attorney told Judge Levy that he "did not know" where the

privileged documents came from.

27. Judge Levy conducted an in-camera review of the documents and determined that they were protected by the attorney-client privilege. Judge Levy ordered Knox Ricksen to turn over the document to Reyes & Barsoum and instructed Knox Ricksen's attorneys that they were ethically required to conduct a diligent search and notify Reyes & Barsoum if there were additional copies of the document and, if so, to turn them over to Reyes & Barsoum.

28. At no time during the session with Judge Levy did the attorneys for Knox Ricksen inform Judge Levy or Reyes & Barsoum that Knox Ricksen was in possession of tens of thousands of files of other attorney-client files.

29. Plaintiff's intake packet was among the 33 000 thousand files unlawfully accessed and downloaded by the Hacking Defendants' in a same manner as Hector Casillas's In-Take packet.

Defendants' Admitted Unlawful Downloading of Thousands of Confidential Files

30. On or about November 2014, Jorge Reyes had a telephonic discussion with attorney Danowitz from Knox Ricksen. During that conversation, attorney Danowitz admitted that the Casillas In-Take Packet had been downloaded from the HQSU website, along with thousands of other files, and further boasted that he even had a videotape of the method used to accessing the confidential documents from

HQSU.

31. The videotape of the method used to access the confidential documents from the HQSU website depicts Defendant Reynolds scrolling down a list of files where Plaintiff's file is one of the files on that list which was later downloaded.

32. Plaintiff's home address, telephone numbers, birth date, Social Security number, email address, legal status, drivers license information, medical information, employment information, salary information and personal information unlawfully became in the possession of the "Hacking defendants" and may even be now in the hands of criminals sold on the "black market".

Defendants' Conspiracy to Violate State and Federal Computer Security Laws

33. Defendants Reynolds and Glover are private investigators. Reynolds was employed by and/or acted as an agent for BHHC, and continues to hold himself out as employed by BHHC. Oliver Glover was and is employed by defendant Zenith.

34. At the direction of BHHC and Zenith and possibly others presently unknown, Reynolds and Glover intentionally implemented a scheme to wrongfully engage in a continuous pattern of cyberattacks over a period of years to access, obtain, retain, and use thousands of attorney-client privileged documents of claimants and their attorneys in litigation in order to gain a litigation advantage and

save huge sums in judgments or settlements. Moreover such information was easily available to be sold to the "black market" for financial gain.

35. In a Declaration provided by Reynolds in Casillas v. Xerxes Corp., et al., California Workers Compensation Appeals Board Case No. AD 19030735, Reynolds admits that he is a private investigator, and that he and Glover participated in downloading from HQ Sign Up "approximately 32,500 intake sheets".

36. Defendant Glover likewise admitted in a sworn deposition in Reyes & Barsoum, LLP v. Knox Ricksen, LLP, et al., Case No. BC 572975 (Superior Court of California, County of Los Angeles), that he had accessed HQSU's server and downloaded over 32,000 workers' compensation files. In that deposition testimony, Glover testified that he first became aware of HQSU in October of 2012, and that he was unable to access the server at that time.

37. Glover went on to testify that Defendant Zenith's counsel was aware of and approved his continued attempts to access the site. With the assistance of Zenith's information technology department, Glover was able to unlawfully access and download files some 500 times in 2012 and 2013 and 2014.

38. The unlawful accessing and downloading of Plaintiff's and others' files took place prior to any litigation being filed, and was entirely independent of any litigation or other protected activity.

39. On information and belief, all defendants have conspired with one

another, and aided and abetted one another, to hack the litigation files of Plaintiff and those of the proposed class members. The cyberattacks were planned and executed by all defendants and the wrongfully obtained privileged information was compromised by each of them to the detriment of plaintiff and the proposed class members.

40. On November 24, 2014, in a second hearing regarding Mr. Casillas, attorney Danowitz again admitted to downloading and possessing over 33,000 attorney files and documents. Moreover, attorney Danowitz now admitted to being in possession of a thumb drive containing the 33,000 files.

41. During this second meeting on November 24, 2014, Danowitz showed a video he recorded demonstrating defendant Reynolds illegally downloading the privileged documents from the HQSU website.

42. The video clearly displays the illegal cyberattack, which Plaintiff’s experts have identified as a directory traversal attack. Directory traversal is an HTTP exploit which allows attackers to access restricted directories and execute commands outside of the web server’s root directory.

43. Danowitz admitted that this conduct was intentional and not inadvertent or accidental.

44. Defendants each conspired with one another, and aided and abetted one another, to unlawfully obtain, publish and use the illegally obtain confidential files of plaintiff and those similarly situated to obtain an advantage in litigation, to

diminish the financial exposure of the named defendant insurance companies and/or to sell that information on the "black market" for profit.

45. The Hacking Defendants, and each of them, knew that they were engaged in tortious and criminal conduct in furtherance of their conspiracy. Each knew that members of the conspiracy were illegally obtaining confidential files and holding them for use against adverse litigants or for financial gain.

46. Each of the hacking defendants, who are each co-conspirators, aided and abetted the commission of the computer crimes enumerated in this Complaint as well as the commission of intentional torts also enumerated in this Complaint. They each provided substantial assistance or encouragement to the other co-conspirators to commit theft of confidential files stored on a computer system and to then distribute those files for their commercial advantage.

COUNT ONE

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030,et seq.)

(Against All Hacking Defendants)

47. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

48. The computers, computer networks, and computer services which stored Plaintiff's personal and privileged information are "protected computers" as defined in 18 U.S.C. § 1030(e)(2), and contain private and confidential information

which affects interstate commerce.

49. Federal law prohibits anyone from "intentionally accesses[ing] a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution." 18 U.S.C. § 1030(a)(2).

50. As alleged in detail above, the Hacking Defendants intentionally and without authorization accessed Plaintiff's personal and confidential information on those protected computers and servers and obtained confidential information, in violation of 18 U.S.C. § 1030(a)(2)(C).

51. The Hacking Defendants' unlawful conduct has caused Plaintiff to suffer substantial loss or damages in an amount to be proven at trial but which during a one-year period aggregates to at least $5,000, and Defendants' conduct causes a threat to public safety. 18 U.S.C. §1030 (a)(5)(A), (B)(i) and (iv), (C).

52. The Hacking Defendants' activity occurred within the last four (4) years from the initiation of this litigation and constitutes a violation of the Computer Fraud and Abuse Act, 18 U.S. C. § 1030(g), and Plaintiff is entitled to damages and injunctive and equitable relief against Defendants under the Act.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Enter judgment in favor of Plaintiff and against the Hacking Defendants in an amount sufficient to compensate Plaintiff for her actual damages;

(b) Afford Plaintiff a trial by jury;

(c) Enjoin the Hacking Defendants from accessing without authorization HQSU's computers and Plaintiff's electronic information;

(d) Destroy or return to Plaintiff any unlawfully obtained information; and

(e) Such other and further relief that this Court deems just and proper.

COUNT TWO

(Violation of the Unlawful Access to Stored Communications Act, 18 U.S.C. § 2701, et seq.)

(Against All Hacking Defendants)

53. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

54. The federal Stored Communications Act ("SCA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . ." 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(12).

55. Pursuant to the SCA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their recipient.

56. Congress enacted the SCA to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99-541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

57. As such, the SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization. 18 U.S.C. § 2701(a).

58. The Hacking Defendants violated 18 U.S.C. § 2701(a)(1) by intentionally accessing Plaintiff's communications without authorization and obtaining and/or altering authorized access to a wire or electronic communication while in electronic storage, as alleged in detail above.

59. The Hacking Defendants violated 18 U.S.C. § 2701(a)(2) because they intentionally exceeded authorization to access Plaintiffs' communications and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage.

60. As a result of the Hacking Defendants' conduct described herein, and its violation of § 2701, Plaintiff has suffered substantial injuries and damage.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Enjoin the Hacking Defendants' conduct described herein;

(b) Award the maximum statutory and punitive damages available under 18 U.S.C. § 2707; and

(c) Such other and further relief that this Court deems just and proper.

COUNT THREE
(Violation of the Electronic Communications Privacy Act, 18 U.S.C.§ 2510, et seq.)

(Against All Hacking Defendants)

61. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

62. The Electronic Communications Privacy Act,18 U.S.C. § 2510et seq. ("ECPA") defines "electronic communications system" as any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communication, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

63. The ECPA broadly defines the "contents" of a communication, when used with respect to any wire, oral, or electronic communications, to include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

64. The Hacking Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally accessing, intercepting, and converting Plaintiff's wire and/or electronic

communications to, from, and within HQSU's computers and servers, as alleged in detail above.

65. The Hacking Defendants also violated 18 U.S.C. § 2511(1)(d) by intentionally using, and endeavoring to use the contents of Plaintiff's wire and/or electronic communications to profit from their unauthorized and unlawful activities.

66. The Hacking Defendants intentionally obtained and/or intercepted, by device or otherwise, these wire and/or electronic communications, without the knowledge, consent or authorization of Plaintiff.

67. Plaintiff suffered harm as a result of the Hacking Defendants' violations of the ECPA.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Grant preliminary, equitable and declaratory relief as may be appropriate;

(b) Award the sum of the actual damages suffered and the profits obtained by the Hacking Defendants as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater; and

(c) Award punitive damages and reasonable costs and attorneys' fees.

COUNT FOUR
(Invasion of Privacy – Public Disclosure of Private Facts)

(Against All Hacking Defendants)

68. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the

allegations.

69. As alleged in detail above, the Hacking Defendants published or caused to be published to the public private facts concerning Plaintiff, including personal and medical information.

70. The published facts were not of legitimate public concern, and the publication would be offensive and objectionable to a reasonable person and was offensive and objectionable to Plaintiff.

71. The Hacking Defendants acted with reckless disregard for the fact that a reasonable person would find the invasion highly offensive.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Enter judgment in favor of Plaintiff on the claim of invasion of privacy;

(b) Award such compensatory as may be proven at trial;

(c) Award punitive damages in an amount sufficient to punish and deter the Hacking Defendants in the future; and

(d) Award such other and further relief as is just and appropriate.

COUNT FIVE

(Violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, et seq.)

(Against All Hacking Defendants)

72. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

73. Plaintiff is the owner and rights, title, and interest in certain data contained in the computer systems and servers owned and operated by HQSU pursuant to § 502(b)(3), § 502(b)(6) and § 502(2)(1).

74. Defendants have violated California's Computer Crime law, including but not limited to § 502(c)(1)(B), by knowingly accessing and without permission obtaining property or data.

75. Defendants have violated California's Computer Crime law, including but not limited to § 502(c)(2), and (7) by knowingly accessing and without permission making use of data from a computer, computer system, or computer network.

76. Defendants have violated California's Computer Crime law, including but not limited to § 502(c)(4), by knowingly accessing and without permission obtaining property or data.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Enter judgment in favor of Plaintiff on the claim of Violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, et seq. pursuant to § 502(e)(1)-(2);

(b) Award such compensatory as may be proven at trial;

(c) Enjoin any further violations of the California Computer Data Access and Fraud Act;

(d) Award attorney's fees;

(e) Order that Defendants forfeit all data owned by Plaintiff unlawfully obtained by Defendants; and

(f) Award such other and further relief as is just and appropriate.

COUNT SIX
(Violation of California Business and Professions Code § 17200)

(Against All Hacking Defendants)

77. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

78. This cause of action is brought pursuant to California Unfair Competition Law at Business & Professions Code § 17200, et seq.

79. Defendants' conduct constitutes unfair, unlawful and/or fraudulent business practices within the meaning of Business & Professions Code § 17200.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Pursuant to Business & Professions Code § 17203, Defendants, and each of them, be ordered to make restitution and disgorge all earnings, profits, compensation, benefits and other ill-gotten gains obtained by Defendants as a result of Defendants' conduct in violation of Business & Professions Code § 17200, et seq.;

(b) Pursuant to Business & Professions Code § 17204, enjoin Defendants, and each of them, from continuing to engage in the acts as set forth in this Complaint, which acts constitute violations of Business & Professions Code § 17200 et seq. Plaintiff will be irreparably harmed if such an order is not granted; and

(c) Award such other and further relief as the Court deems just and proper.

COUNT SEVEN
(Conversion)

(Against All Hacking Defendants)

80. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

81. As alleged in detail herein, Plaintiff owned the privileged and confidential information and data relating to her workers compensation claim.

82. Defendants intentionally and substantially interfered with Plaintiff's property by unlawfully accessing and downloading copies of that data.

83. Plaintiff did not consent to Defendants' activity, as alleged herein.

84. Plaintiff was injured as a result of Defendants' unlawful conversion in an amount to be proven at trial.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Award compensatory general and special damages pursuant to Cal. Civ. Code § 3336;

(b) Award Plaintiff's costs and fees, including attorney's fees, in bringing this action; and

(c) Award such other and further relief as the Court deems just and proper.

COUNT EIGHT
(Negligence)

(Against HQSU)

85. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

86. Defendant HQSU owed a duty to Plaintiff to exercise reasonable care in obtaining, securing, safeguarding, and protecting Plaintiff's confidential and privileged information in its possession and to prevent it from being compromised, accessed, stolen, and used by unauthorized persons.

87. This duty included, among other things, designing and maintaining a security system that ensured Plaintiff's data was adequately secured and protected. HQSU further owed Plaintiff a duty to implement processes that detected breaches of its security system in a timely manner and to timely act upon security breaches, including notifying Plaintiff that her private data had been compromised.

88. HQSU owe Plaintiff a duty of care to because Plaintiff was a foreseeable and probable victim of any inadequate security practices. HQSU knew or should have known it had inadequately safeguarded its network, yet failed to take reasonable precautions against security breaches.

89. HQSU owed a duty to timely and accurately disclose to Plaintiff its

computer server had been or reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiff could take appropriate measures to avoid identity theft or fraud.

90. Plaintiff relied on and entrusted HQSU with confidential, private, and privileged information, and HQSU was in a position to prevent unlawful access to that data through the use of adequate and responsible security measures.

91. HQSU had a duty to take reasonable measures to protect and safeguard Plaintiff's data.

92. HQSU breached that duty by negligently, grossly negligently, and wantonly failing to take reasonable and adequate measure to secure and safeguard Plaintiff's confidential information, and then by failing to inform Plaintiff when it became aware that the information had been compromised.

93. Plaintiff suffered and continues to suffer harm has a direct and proximate result of HQSU's negligence and gross negligence.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Award Plaintiff compensatory general and special damages;

(b) Award Plaintiff punitive damages as a result of HQSU's gross negligence and wanton conduct;

(c) Award Plaintiff's costs and fees, including attorney's fees, in bringing this action; and

(d) Award such other and further relief as the Court deems just and proper.

COUNT NINE

(Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code§ 56, et seq.)

(Against HQSU)

94. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

95. California Civil Code§ 56,etseq., known as the Confidentiality of Medical Information Act (“Medical Information Act”), requires companies which Receive medical information to establish appropriate procedures to ensure the Confidentiality and protection from unauthorized use and disclosure of that information.

96. At all relevant times, HQSU had a legal duty to protect the confidentiality of Plaintiff’s confidential and privileged information, which included medical information.

97. By failing to ensure adequate security systems were in place to Prevent access and disclosure of Plaintiff’s private medical information without written authorization, HQSU violated the Medical Information Act and its legal duty to protect the confidentiality of such information.

98. Pursuant to Cal. Civ. Code § 56.36, Plaintiff is entitled to nominal damages and statutory damages of $1,000, as well as Plaintiff’s actual damages as proven at trial.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Award Plaintiff nominal and statutory damages of $1000.00;

(b) Award Plaintiff compensatory damages for actual harm suffered;

(c) Award Plaintiff's costs and fees, including attorney's fees, in bringing this action; and

(d) Award such other and further relief as the Court deems just and proper.

COUNT TEN

(Violation of California Data Security and Breach Notification Act, Cal. Civ. Code § 1798.80, et seq.)

(Against HQSU)

99. Plaintiff incorporates each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations.

100. The California Data Security and Breach Notification Act, Cal. Civ. Code § 1798.80, et seq. (the "Data Security Act") provided, at the time relevant to the acts and omissions in this Complaint, that businesses which hold private and confidential information of California residents must implement and maintain reasonable security measures to protect personal data about those residents. Id., § 1798.81.5.

101. The personal information protected by the Data Security Act includes a resident's first name or initial and last name, in combination with one or more of the following: (i) social security number; (ii) driver's license; (iii) account number,

credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; or (iv) medical information – i.e., individually identifiable information about an individual's medial history, medical treatment or diagnosis by a health care professional.

102. In addition to requiring adequate security measures, the Act also requires that the affected resident be notified in the event of a data security breach.

103. HQSU violated each of these provisions by failing to provide adequate security measures and failing to notify Plaintiff after learning that HQSU's system had been breached and Plaintiff's confidential information had been compromised.

WHEREFORE, Plaintiff respectfully requests that this Court:

(a) Award Plaintiff nominal and statutory damages of $1000.00;

(b) Award Plaintiff compensatory damages for actual harm suffered;

(c) Award Plaintiff's costs and fees, including attorney's fees, in bringing this action; and

(d) Award such other and further relief as the Court deems just and proper.

CLASS ACTION ALLEGATIONS

104. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and the classes preliminarily defined as:

Nationwide Class

105. Current and former persons whose legal files were unlawfully accessed

and downloaded by Defendants.

106. Excluded from the proposed classes are anyone employed by counsel for Plaintiff in this action and any Judge to whom this case is assigned, as well as her or her staff and immediate family.

107. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

108. Numerosity. The proposed class consists of thousands of persons nationwide whose legal files were unlawfully and without authorization accessed and downloaded by Defendants, including between 3000 to 5000 former and current clients of Reyes & Barsoum, as well as tens of thousands of other individuals, who had their data stolen by defendants' conduct as described above, making joinder of each individual class member impracticable.

109. Commonality. Common questions of law and fact exist for the proposed class' claims and predominate over questions affecting only individual class members. Common questions include:

a. Whether defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. §§1030 et seq.;

b. Whether defendants violated the Unlawful Access to Stored Communications Act, 18 U.S.C. §§2701 et seq.;

c. Whether defendants violated the California Business and Professions Code

§§17200, et seq.;

d. Whether defendants violated the California Computer Data Access and Fraud Act, California Penal Code §§502, et seq.;

e. Whether defendants invaded the privacy of the class members;

f. Whether defendants intentionally interfered with the class members' prospective economic advantages.

110. Typicality. Plaintiff's claims are typical of the claims of the proposed classes because, among other things, Plaintiff and class members sustained similar injuries as a result of defendants' wrongful conduct and their legal claims all arise from the intentional and illegal cyberattack on their legal files.

111. Adequacy. Plaintiff will fairly and adequately protect the interests of the classes. her interests do not conflict with class members' interests and he has retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the classes.

112. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent

or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action devise presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

113. In addition, class certification is appropriate under Rule 23(b)(1) or (b)(2) because:

a. The prosecution of separate actions by the individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for defendants;

b. The prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Defendants have acted or have refused to act on grounds that apply generally to the proposed class, thereby making final injunctive relief described herein appropriate with respect to the proposed class as a whole.

PRAYER FOR RELIEF

(On All Causes of Action)

WHEREFORE, Plaintiff prays that the Court:

1. Certify a nationwide class of Plaintiffs affected and injured by Defendants'

unlawful conduct as alleged herein;

2. Enter judgment in favor of Plaintiff and against the Defendants.

3. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression.

4. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

5. Enter a preliminary and permanent injunction prohibiting Defendants from accessing, downloading, or otherwise using any data or information from HQSU's computer systems or any other system housing Plaintiff's privileged and confidential material.

6. Enter judgment awarding Plaintiff actual damages from Defendants adequate to compensate Plaintiff for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

7. Enter judgment in favor of Plaintiff disgorging Defendants' profits.

8. Enter judgment in favor of Plaintiff awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

9. Enter judgment in favor of Plaintiff awarding attorneys' fees and costs, and;

10. Order such other relief that the Court deems just and reasonable.

Respectfully Submitted,

Dated: April 19, 2016

LAW OFFICE OF MARK RAVIS & ASSOCIATES

/s/ David Martin

David Martin
Attorneys for Plaintiff & Proposed Class